APDUs

EXTERNAL AUTHENTICATE command

Practical exercises

1. Looking at Trace 01 (in file “01.10 EXTERNAL AUTHENTICATE command - Trace 01.txt”).

   a. What does Byte 1, bit 3 of the Application Interchange Profile (tag 82), returned by the card in the response to the GET PROCESSING OPTIONS command, indicate?

   ____

   b. What is the implication for the transaction flow?

   ____

   c. Between which commands is the EXTERNAL AUTHENTICATE command located?

   ____

   d. What is the header of the EXTERNAL AUTHENTICATE command?

   ____

e. How many bytes of data does the terminal send with the EXTERNAL AUTHENTICATE command? Those constitute the Issuer Authentication Data, sent as tag 91 by the issuer to the terminal.

____

f. In those data, what is the ARPC (Authorization Response Cryptogram)?

____

g. In those data, what is the Response code?

____

h. What Status Word does the card return to the EXTERNAL AUTHENTICATE command?

____

i. What does it mean?

____

j. What type of cryptogram does the card return in response to the second GENERATE AC command?

____

2. Now looking at Trace 02 (in file "01.10 EXTERNAL AUTHENTICATE command - Trace 02.txt").

   a. What Status Word does the card return to the EXTERNAL AUTHENTICATE command?

   ____

   b. What does it mean?

   ____

c. What type of cryptogram does the card return in response to the second GENERATE AC command?

____

Answers

1.a. From 82-02-5C00, Byte 1, bit 3 is set to 1. This indicates that Issuer authentication is supported.

1.b. The implication is that, if the issuer returns an ARPC (response cryptogram), the terminal will need to use the dedicated EXTERNAL AUTHENTICATE command to present it to the card

1.c. The EXTERNAL AUTHENTICATE command is located between the first and the second GENERATE AC command. In essence, the terminal asks the card to validate the issuer response cryptogram before it asks the card for a second decision.

1.d. The header of the EXTERNAL AUTHENTICATE command is 008200000A

1.e. The terminal sends 10 bytes (0x0A) with the EXTERNAL AUTHENTICATE command

1.f. The ARPC (Authorization Response Cryptogram) is 8D335A8E0372F989

1.g. The Response code is 3030. This is a VISA card, the response code in tag 91 is just a repeat of the value in tag 8A in the second GENERATE AC command.

1.h. The card returns Status Word 9000 to the EXTERNAL AUTHENTICATE command.

1.i. It indicates a successful return from External Authenticate. The card checked the ARPC value, and found it to be authentic.

1.j. From 9F27-01-40, the card produced a TC (approval). This is a true online approval, as it follows the validation of the issuer response in the EXTERNAL AUTHENTICATE command.

2.a. The card returned Status Word 6300 to the EXTERNAL AUTHENTICATE command.

2.b. It means “Issuer Authentication Data verification failed”. The card rejected the ARPC (response cryptogram) presented by the terminal. Technically, this indicates that the ARPC was either enciphered with the wrong key, or that there is a discrepancy between the response code presented to the card (here 3030 - Approval) and the response code that the issuer used as an input to the ARPC generation.

2.c. From 9F27-01-00, the card produced an AAC (decline). In this instance, the failure of ARPC verification caused the card to decline the transaction.

Note that this is not automatic, it depends on card settings (which are not visible to the terminal). An issuer may decide to set up cards so that ARPC verification failure does not cause a decline, but that cards will instead consider the transaction as being offline (and make use of their internal counters). This is a matter of cardholder risk profile, and reliability of communications.